AO 93C (08/18) Warrant by Telephone or Other Reliable Electronic Means

❒ Original

CLERK'S OFFICE
A TRUE COPY
Sep 02, 2020
s/ JeremyHeacox
Deputy Clerk, U.S. District Court
Eastern District of Wisconsin

# UNITED STATES DISTRICT COURT

for the

Eastern District of Wisconsin

In the Matter of the Search of
*(Briefly describe the property to be searched or identify the person by name and address)*
information associated with five Apple IDs and Apple iCloud accounts that is stored at premises controlled by Apple

Case No. 20-M-356 (SCD)

## WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search and seizure of the following person or property located in the _____ District of _____
*(identify the person or describe the property to be searched and give its location)*:

See Attachment A.

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal *(identify the person or describe the property to be seized)*:

See Attachment B.

**YOU ARE COMMANDED** to execute this warrant on or before 9-15-2020 *(not to exceed 14 days)*

❒ in the daytime 6:00 a.m. to 10:00 p.m. ☑ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to Stephen C. Dries.
*(United States Magistrate Judge)*

❒ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized *(check the appropriate box)*

❒ for _____ days *(not to exceed 30)* ❒ until, the facts justifying, the later specific date of _____.

Date and time issued: 9-2-2020 11:40

Stephen C. Dries
*Judge's signature*

City and state: Milwaukee, Wisconsin

Stephen C. Dries, U.S. Magistrate Judge
*Printed name and title*

**Return**

| Case No.: | Date and time warrant executed: | Copy of warrant and inventory left with: |
|---|---|---|

Inventory made in the presence of :

Inventory of the property taken and name(s) of any person(s) seized:

**Certification**

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: _____

_____
*Executing officer's signature*

_____
*Printed name and title*

## ATTACHMENT A

### Property to Be Searched

This warrant applies to information associated with the Apple IDs and Apple iCloud accounts associated with the following information, that is stored at premises owned, maintained, controlled, or operated by Apple Inc., a company headquartered at Apple Inc., One Apple Park Way, Cupertino, California 95014.

**Account 1:**

- Name: Jaquan D. Moore
- Date of birth: 10/04/1997
- Address: 119 16th Avenue NE, Minneapolis, Minnesota 55413

**Account 2:** Phone: (612) 802-8429

**Account 3:** JDEEL08@ICLOUD.COM

**Account 4:** JDEEL08@YAHOO.COM

**Account 5:** Phone: (612) 513-9131

## ATTACHMENT B

### Particular Things to be Seized

### I. Information to be disclosed by Apple

To the extent that the information described in Attachment A is within the possession, custody, or control of Apple, regardless of whether such information is located within or outside of the United States, including any messages, records, files, logs, or information that have been deleted but are still available to Apple, or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Apple is required to disclose the following information to the government, in unencrypted form whenever available, for each account or identifier listed in Attachment A:

a. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers, email addresses (including primary, alternate, rescue, and notification email addresses, and verification information for each email address), the date on which the account was created, the length of service, the IP address used to register the account, account status, associated devices, methods of connecting, and means and source of payment (including any credit or bank account numbers);

b. All records or other information regarding the devices associated with, or used in connection with, the account (including all current and past trusted or authorized iOS devices and computers, and any devices used to access Apple services), including serial numbers, Unique Device Identifiers ("UDID"), Advertising Identifiers ("IDFA"), Global Unique Identifiers ("GUID"), Media Access Control ("MAC") addresses, Integrated Circuit Card ID numbers ("ICCID"), Electronic Serial Numbers ("ESN"), Mobile Electronic Identity Numbers ("MEIN"), Mobile Equipment Identifiers ("MEID"), Mobile Identification Numbers ("MIN"), Subscriber Identity Modules ("SIM"), Mobile Subscriber Integrated Services Digital Network Numbers

("MSISDN"), International Mobile Subscriber Identities ("IMSI"), and International Mobile Station Equipment Identities ("IMEI");

c. The contents of all emails associated with the account from August 22, 2020 through September 1, 2020, including stored or preserved copies of emails sent to and from the account (including all draft emails and deleted emails), the source and destination addresses associated with each email, the date and time at which each email was sent, the size and length of each email, and the true and accurate header information including the actual IP addresses of the sender and the recipient of the emails, and all attachments;

d. The contents of all instant messages associated with the account from August 22, 2020 through September 1, 2020, including stored or preserved copies of instant messages (including iMessages, SMS messages, and MMS messages) sent to and from the account (including all draft and deleted messages), the source and destination account or phone number associated with each instant message, the date and time at which each instant message was sent, the size and length of each instant message, the actual IP addresses of the sender and the recipient of each instant message, and the media, if any, attached to each instant message;

e. The contents of all files and other records stored on iCloud, including all iOS device backups, all Apple and third-party app data, all files and other records related to iCloud Mail, iCloud Photo Sharing, My Photo Stream, iCloud Photo Library, iCloud Drive, iWork (including Pages, Numbers, Keynote, and Notes), iCloud Tabs and bookmarks, and iCloud Keychain, and all address books, contact and buddy lists, notes, reminders, calendar entries, images, videos, voicemails, device settings, and bookmarks;

f. All activity, connection, and transactional logs for the account (with associated IP addresses including source port numbers), including FaceTime call invitation logs, messaging and

query logs (including iMessage, SMS, and MMS messages), mail logs, iCloud logs, iTunes Store and App Store logs (including purchases, downloads, and updates of Apple and third-party apps), My Apple ID and iForgot logs, sign-on logs for all Apple services, Game Center logs, Find My iPhone and Find My Friends logs, logs associated with web-based access of Apple services (including all associated identifiers), and logs associated with iOS device purchase, activation, and upgrades;

g. All records and information regarding locations where the account or devices associated with the account were accessed, including all data stored in connection with Location Services, Find My iPhone, Find My Friends, and Apple Maps;

h. All records pertaining to the types of service used;

i. All records pertaining to communications between Apple and any person regarding the account, including contacts with support services and records of actions taken; and

j. All files, keys, or other information necessary to decrypt any data produced in an encrypted form, when available to Apple (including, but not limited to, the keybag.txt and fileinfolist.txt files).

Apple is hereby ordered to disclose the above information to the government within **10 DAYS** of issuance of this warrant.

## II. Information to be seized by the government

All information described above in Section I that constitutes evidence of travel in interstate commerce or use of a facility of interstate commerce with intent to riot, in violation of Title 18, United States Code, Section 2101, conspiracy to commit arson, in violation of Title 18, United States Code, Section 844(m), arson of commercial property, in violation of Title 18, United States Code, Section 844(i), burglary involving controlled substances, in violation of Title 18, United States Code, Section 2118(b), conspiracy to commit burglary involving controlled substances, in violation of Title 18, United States Code, Section 2118(d), false statements, in violation of Title 18, United States Code, Section 1001, and destruction, alteration, or falsification of records in federal investigations, in violation of Title 18, United States Code, Section 1519, involving Jaquan D. Moore, Jada Deel, and others since August 22, 2020, including, for each account or identifier listed on Attachment A, information pertaining to the following matters:

a. Preparatory steps taken in furtherance of these crimes;

b. Communications between Jaquan D. Moore, Jada Deel, Sherwin Pompey, James L. Fielders-Bowers, or others;

c. Relationship between Jaquan D. Moore, Jada Deel, Sherwin Pompey, James L. Fielders-Bowers, or others;

d. Information about the protests, riots, and civil unrest in the Kenosha, Wisconsin area occurring between August 23, 2020 and September 1, 2020;

e. Use, possession, custody, or control of the phone numbers 612-802-8429, 612-513-9131, 612-735-7080, and 262-653-6404;

f. Use, possession, custody, control, or location of the cellular device assigned International Mobile Subscriber Identity (IMSI) 310410231756520;

g. Use, possession, custody, control, or location of a Dodge Charger, a black Nissan Rogue SUV, and a white four-door Pontiac sedan

h. Accelerants or ignitable liquids (such as gasoline, kerosene, or other petroleum distillates), glass bottles, ignition devices (such as an improvised wick or towel), heat sources, and ignition sources (such as a lighter or matches);

i. Screwdriver, hammer, or other burglar's tools;

j. Appearance, clothing, and identity of Jaquan D. Moore on August 24, 2020;

k. Charlie's 10th Hole bar, located at 3805 22nd Avenue, Kenosha, Wisconsin;

l. CVS pharmacy, located at 3726 22nd Avenue, Kenosha, Wisconsin 53140;

m. Location, whereabouts, and patterns of travel of Jaquan D. Moore, Jada Deel, and others;

n. The identity of the person(s) who created or used the Apple ID, including records that help reveal the whereabouts of such person(s);

o. Any information about the existence, scope, or overt acts in furtherance of a conspiracy;

p. Any information related to motive, intent, or knowledge of the violations described above;

q. Any information related to the concealment or destruction of evidence of the violations described above;

r. Evidence indicating how and when the account was accessed or used, to determine the chronological and geographic context of account access, use and events relating to the crime under investigation and the account subscriber;

s. Any records pertaining to the means and source of payment for services (including any credit card or bank account number or digital money transfer account information);

t. Evidence indicating the subscriber's state of mind as it relates to the crime under investigation; and

u. Evidence that may identify any co-conspirators or aiders and abettors, including records that help reveal their whereabouts.

# UNITED STATES DISTRICT COURT

for the

Eastern District of Wisconsin

In the Matter of the Search of
*(Briefly describe the property to be searched or identify the person by name and address)*

information associated with five Apple IDs and Apple iCloud accounts that is stored at premises controlled by Apple

Case No. 20-M-356 (SCD)

## APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

See Attachment A.

located in the _____ District of _____, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☐ contraband, fruits of crime, or other items illegally possessed;
- ☐ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

| *Code Section* | *Offense Description* |
|---|---|
| 18 U.S.C. 2101, 844(n), 844(i), 2118(b), 2118(d), 1001, and 1519 | travel in interstate commerce or use of a facility with intent to riot, arson conspiracy, arson, burglary involving controlled substances, burglary conspiracy, false statements, and destruction, alteration, or falsification of records |

The application is based on these facts:

See the attached affidavit.

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days *(give exact ending date if more than 30 days:* _____ *)* is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

RICHARD CONNORS Digitally signed by RICHARD CONNORS Date: 2020.09.02 11:10:54 -05'00'

*Applicant's signature*

Richard E. Connors III, Special Agent (ATF)

*Printed name and title*

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone *(specify reliable electronic means).*

Date: 09/02/2020

Stephen C. Dries

*Judge's signature*

City and state: Milwaukee, Wisconsin

Stephen Dries

*Printed name and title*

**AFFIDAVIT IN SUPPORT OF**
**AN APPLICATION FOR A SEARCH WARRANT**

I, Richard Connors, being first duly sworn, hereby depose and state as follows:

## INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Apple Inc. (hereafter "Apple") to disclose to the government records and other information, including the contents of communications, associated with the Apple IDs and Apple iCloud accounts associated with the following information, further described in Attachment A, that is stored at premises owned, maintained, controlled, or operated by Apple, a company headquartered at One Apple Park Way, Cupertino, California 95014:

**Account 1:**

- Name: Jaquan D. Moore
- Date of birth: 10/04/1997
- Address: 119 16th Avenue NE, Minneapolis, Minnesota 55413

**Account 2:** Phone: (612) 802-8429

**Account 3:** JDEEL08@ICLOUD.COM

**Account 4:** JDEEL08@YAHOO.COM

**Account 5:** Phone: (612) 513-9131

2. The information to be disclosed by Apple and searched by the government is described in the following paragraphs and in Attachments A and B.

3. I am employed as a Special Agent with the United States Department of Justice's Bureau of Alcohol, Tobacco, Firearms and Explosives ("ATF") assigned to the Milwaukee Field Office since October 2015. I have been employed as a full time law enforcement officer for approximately four and a half years. I have received training at the Federal Law Enforcement

Training Center in Glynco, Georgia. I attended the Criminal Investigator Training Program, as well as ATF's Special Agent Training Program. I have received training in the investigation of arsons. Prior to becoming a Special Agent with the ATF, I received two bachelor's degrees from Northern Illinois University in the fields of Sociology and International Relations. I have received a master's degree from Northern Illinois University in the field of American Government.

4. As an ATF agent, I have been deployed to assist with riots involving arsons, including the riots in the Sherman Park neighborhood of Milwaukee in 2016. I know from training and experience that those that commit arsons during riots commonly communicate, photograph, videotape, and organize using electronic devices, including by phone call, text message, electronic mail, messaging application, and social media.

5. I am an investigative or law enforcement officer of the United States within the meaning of Section 2510(7) of Title 18, United States Code, in that I am empowered by law to conduct investigations of and to make arrests for federal offenses. As a part of my duties with the ATF, I investigate criminal violations relating to arson and arson-related offenses, including violations of Title 18, United States Code, Section 844. During the course of my investigations, I have regularly used electronic evidence relating to the commission of criminal offenses, including intent, motive, manner, means, and the identity of co-conspirators.

6. The facts in this affidavit come from my personal observations, my training and experience, and information provided to me by other federal, state, and local law enforcement officers and other witnesses. This affidavit is intended to show simply that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

7. Based on the facts as set forth in this affidavit, there is probable cause to believe that the information described in Attachment A contains evidence of travel in interstate commerce or use of a facility of interstate commerce with intent to riot, in violation of Title 18, United States Code, Section 2101, conspiracy to commit arson, in violation of Title 18, United States Code, Section 844(n), arson of commercial property, in violation of Title 18, United States Code, Section 844(i), burglary involving controlled substances, in violation of Title 18, United States Code, Section 2118(b), conspiracy to commit burglary involving controlled substances, in violation of Title 18, United States Code, Section 2118(d), false statements, in violation of Title 18, United States Code, Section 1001, and destruction, alteration, or falsification of records in federal investigations, in violation of Title 18, United States Code, Section 1519, as described in Attachment B.

## JURISDICTION

8. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A), & (c)(1)(A). Specifically, the Court is "a district court of the United States . . . that has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i).

## PROBABLE CAUSE

9. On August 23, 2020, Jacob Blake was shot multiple times by officers of the Kenosha Police Department. That incident triggered both non-violent protests and violent rioting, including numerous arsons throughout the City of Kenosha. The unrest and violence grew so dangerous that the Wisconsin National Guard eventually deployed over 1,000 individuals to keep the peace. The Government also marshaled its resources to investigate various crimes associated with these incidents, including numerous arsons. The ATF, for its part, deployed its National

Response Team of 50 expert arson investigators to Kenosha, who are currently processing scenes, collecting video evidence, and identifying potential subjects. The instant warrant application is made as a part of that response effort.

10. In conjunction with other federal, state, and local law enforcement officers, I am conducting an investigation into an arson at Charlie's 10th Hole bar, located at 3805 22nd Avenue, Kenosha, Wisconsin, on August 24, 2020, and other related crimes. That night, several individuals were captured on surveillance camera outside the bar at the time the fire was set. One individual threw a flaming object through the front window of the bar igniting a fire inside. The ATF and Wisconsin Department of Justice's Division of Criminal Investigations responded and classified the fire as incendiary.

11. On August 24, 2020 at about 11:59 p.m.—shortly after the arson, officers of the Kenosha Police Department arrested Jaquan D. Moore (DOB: 10/04/1997) for a burglary of the CVS pharmacy, located at 3726 22nd Avenue, Kenosha, Wisconsin 53140—across the street from Charlie's 10th Hole Bar. Upon arrival, officers observed the bottom half of CVS's glass sliding doors were shattered and entered the building to check for subjects. Multiple men fled, but officers were able to apprehend Moore, who was wearing a white t-shirt around his head and face to conceal his identity, along with a gray shirt and dark pants. Officers located a silver hammer with a black handle and a flathead screwdriver with a black-and-red handle in the immediate area around Moore. Officers noted that cash drawers and pill bottles were strewn across the floor, and the store was in disarray. The pharmacy section of the CVS had hundreds of pill bottles strewn across the floor, one shelf of medication was tipped over, and the medication refrigerators were opened.

12. For that crime, Moore was charged with burglary, in violation of Wisconsin Statute 943.10(1m)(a), the next day in Kenosha County Case No. 2020CF000973. According to publicly available court records, Moore's full name is Jaquan D. Moore, his date of birth is October 4, 1997, his phone number is (612) 802-8429, and his address is 1014 Rockefeller Lane, Unit 2, Madison, Wisconsin 53704.

13. On August 28, 2020, Special Agent Rick Hankins of the ATF interviewed Moore, who said that he traveled from Madison, Wisconsin to Kenosha, Wisconsin to partake in "the riots." He said that he was standing next to the person who started the fire at Charlie's 10th Hole. Moore said that he left his cell phone in the vehicle of a person known to him as "George." Moore said that the call number assigned to his cell phone is (612) 802-8429. Moore also said that he has known "George" for several years, but did not know "George's" last name or address. Moore said that "George" was from Minnesota, but now lives in Wisconsin. Moore told investigators that "George" would have information useful to the arson investigation and a shooting that occurred that night.

14. On August 28, 2020, the Honorable Mary Wagner of the Kenosha County Circuit Court, signed a search warrant for the historical location information associated with Moore's cell phone number.

15. A preliminary review of the location information from AT&T showed that Moore's phone traveled from Minnesota to Kenosha on or about August 24, 2020, arriving at approximately 2:53 p.m. Moore's cell phone was stationary in Kenosha for several hours at the time of the arson. (He was arrested on August 24, 2020 at approximately 11:59 p.m.) On August 25, 2020 at approximately 12:22 a.m., Moore's cell phone traveled from Kenosha to Minneapolis, Minnesota, arriving at approximately 6:00 a.m. (while Moore was in custody). On August 25, 2020, at approximately 5:21 p.m., the cellular device appeared to have powered off.

16. The subscriber information for Moore's cell phone lists "Jada L Deel" of 10747 Dunkirk Lane North, Maple Grove, Minnesota 55369 with an email address of jdeel08@icloud.com, but lists the user as "J M" of 119 16th Avenue NE, Minneapolis, Minnesota 55413 with a similar contact email jdeel08@yahoo.com. Those records also list the International Mobile Subscriber Identity (IMSI), a unique identifier, for Jaquan Moore's cell phone assigned call number (612) 802-8429 as 310410231756520, and state that call number has been active since July 29, 2020 to the present.

17. On August 30, 2020, I interviewed Moore with Special Agent Rick Hankins, because the historical location information for Moore's cell phone was inconsistent with Moore's initial statement, in that the location information showed that he traveled across state lines from Minnesota to Wisconsin to participate in the riots. He then admitted that he had traveled from the Twin Cities area in a three-car caravan to participate in the riots. He said that he had known some of the others that traveled with him since middle school, but denied knowing their last names. Moore stated he was riding in a brown Dodge Charger, there was a black SUV, and a white four-door sedan.

18. Investigators obtained surveillance video showing the three-car caravan consisting of a brown Dodge Charger, a black Nissan Rogue SUV, and a white four-door Pontiac sedan arriving in Kenosha on August 24, 2020, as Moore stated, carrying approximately 13 people including Moore.

19. According to jail records, Moore called multiple people from jail, including 612-513-9131 listed to Jada Deel of Maple Grove, Minnesota, 612-735-7080 listed to Sherwin Pompey of Eden Prairie, Minnesota, and 262-653-6404 listed to James L. Fielders-Bowers. Based on a preliminary review of those jail calls, Moore called Jada Deel and provided passwords for various accounts, appearing to reference a cell phone with fingerprint access. Moore says that his phone is in possession of someone named Anthony Clay and asked Deel to get his property, including the cell phone, wallet, prescriptions, $500 in coins, and other items. He also appears to direct Deel to delete information from his accounts. During one of those calls with Jada Deel, Moore said that he went into the CVS with others—that the others went in to steal Percocets, but he was the one who was caught. He admitted that he brought a screwdriver with him, but was unable to steal anything. During another jail call, Moore told his mother to hide his gun and drugs.

20. Based on the information above, there is probable cause to believe that the information described in Attachment A contains evidence of travel in interstate commerce or use of a facility of interstate commerce with intent to riot, in violation of Title 18, United States Code, Section 2101, conspiracy to commit arson, in violation of Title 18, United States Code, Section 844(m), arson of commercial property, in violation of Title 18, United States Code, Section 844(i), burglary involving controlled substances, in violation of Title 18, United States Code, Section 2118(b), conspiracy to commit burglary involving controlled substances, in violation of Title 18, United States Code, Section 2118(d), false statements, in violation of Title 18, United States Code, Section 1001, and destruction, alteration, or falsification of records in federal investigations, in

violation of Title 18, United States Code, Section 1519, as described in Attachment B.

## INFORMATION REGARDING APPLE ID AND iCLOUD[1]

21. Apple is a United States company that produces the iPhone, iPad, and iPod Touch, all of which use the iOS operating system, and desktop and laptop computers based on the Mac OS operating system.

22. Apple provides a variety of services that can be accessed from Apple devices or, in some cases, other devices via web browsers or mobile and desktop applications ("apps"). As described in further detail below, the services include email, instant messaging, and file storage:

a. Apple provides email service to its users through email addresses at the domain names mac.com, me.com, and icloud.com.

b. iMessage and FaceTime allow users of Apple devices to communicate in real-time. iMessage enables users of Apple devices to exchange instant messages ("iMessages") containing text, photos, videos, locations, and contacts, while FaceTime enables those users to conduct video calls.

c. iCloud is a file hosting, storage, and sharing service provided by Apple. iCloud can be utilized through numerous iCloud-connected services, and can also be used to store iOS device backups and data associated with third-party apps.

d. iCloud-connected services allow users to create, store, access, share, and synchronize data on Apple devices or via icloud.com on any Internet-connected device. For example, iCloud Mail enables a user to access Apple-provided email accounts on multiple Apple devices and on icloud.com. iCloud Photo Library and My Photo Stream can be used to store and manage images and videos taken from Apple devices, and iCloud Photo Sharing allows the user to share those images and videos with other Apple subscribers. iCloud Drive can be used to store presentations, spreadsheets, and other documents. iCloud Tabs and bookmarks enable iCloud to be used to synchronize bookmarks and webpages opened in the Safari web browsers on all of the user's Apple devices. iWork Apps, a suite of

[1] The information in this section is based on information published by Apple on its website, including, but not limited to, the following document and webpages: "U.S. Law Enforcement Legal Process Guidelines," available at http://images.apple.com/privacy/docs/legal-process-guidelines-us.pdf; "Create and start using an Apple ID," available at https://support.apple.com/en-us/HT203993; "iCloud," available at http://www.apple.com/icloud/; "What does iCloud back up?," available at https://support.apple.com/kb/PH12519; "iOS Security," available at https://www.apple.com/business/docs/iOS_Security_Guide.pdf, and "iCloud: How Can I Use iCloud?," available at https://support.apple.com/kb/PH26502.

productivity apps (Pages, Numbers, Keynote, and Notes), enables iCloud to be used to create, store, and share documents, spreadsheets, and presentations. iCloud Keychain enables a user to keep website username and passwords, credit card information, and Wi-Fi network information synchronized across multiple Apple devices.

e. Game Center, Apple's social gaming network, allows users of Apple devices to play and share games with each other.

f. Find My iPhone allows owners of Apple devices to remotely identify and track the location of, display a message on, and wipe the contents of those devices. Find My Friends allows owners of Apple devices to share locations.

g. Location Services allows apps and websites to use information from cellular, Wi-Fi, Global Positioning System ("GPS") networks, and Bluetooth, to determine a user's approximate location.

h. App Store and iTunes Store are used to purchase and download digital content. iOS apps can be purchased and downloaded through App Store on iOS devices, or through iTunes Store on desktop and laptop computers running either Microsoft Windows or Mac OS. Additional digital content, including music, movies, and television shows, can be purchased through iTunes Store on iOS devices and on desktop and laptop computers running either Microsoft Windows or Mac OS.

23. Apple services are accessed through the use of an "Apple ID," an account created during the setup of an Apple device or through the iTunes or iCloud services. A single Apple ID can be linked to multiple Apple services and devices, serving as a central authentication and syncing mechanism.

24. An Apple ID takes the form of the full email address submitted by the user to create the account; it can later be changed. Users can submit an Apple-provided email address (often ending in @icloud.com, @me.com, or @mac.com) or an email address associated with a third-party email provider (such as Gmail, Yahoo, or Hotmail). The Apple ID can be used to access most Apple services (including iCloud, iMessage, and FaceTime) only after the user accesses and responds to a "verification email" sent by Apple to that "primary" email address. Additional email addresses ("alternate," "rescue," and "notification" email addresses) can also be associated with an Apple ID by the user.

25. Apple captures information associated with the creation and use of an Apple ID. During the creation of an Apple ID, the user must provide basic personal information including the user's full name, physical address, and telephone numbers. The user may also provide means of payment for products offered by Apple. The subscriber information and password associated with an Apple ID can be changed by the user through the "My Apple ID" and "iForgot" pages on Apple's website. In addition, Apple captures the date on which the account was created, the length of service, records of log-in times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to and utilize the account, the Internet Protocol address ("IP address") used to register and access the account, and other log files that reflect usage of the account.

26. Additional information is captured by Apple in connection with the use of an Apple ID to access certain services. For example, Apple maintains connection logs with IP addresses that reflect a user's sign-on activity for Apple services such as iTunes Store and App Store, iCloud, Game Center, and the My Apple ID and iForgot pages on Apple's website. Apple also maintains records reflecting a user's app purchases from App Store and iTunes Store, "call invitation logs" for FaceTime calls, "query logs" for iMessage, and "mail logs" for activity over an Apple-provided email account. Records relating to the use of the Find My iPhone service, including connection logs and requests to remotely lock or erase a device, are also maintained by Apple.

27. Apple also maintains information about the devices associated with an Apple ID. When a user activates or upgrades an iOS device, Apple captures and retains the user's IP address and identifiers such as the Integrated Circuit Card ID number ("ICCID"), which is the serial number of the device's SIM card. Similarly, the telephone number of a user's iPhone is

linked to an Apple ID when the user signs in to FaceTime or iMessage. Apple also may maintain records of other device identifiers, including the Media Access Control address ("MAC address"), the unique device identifier ("UDID"), and the serial number. In addition, information about a user's computer is captured when iTunes is used on that computer to play content associated with an Apple ID, and information about a user's web browser may be captured when used to access services through icloud.com and apple.com. Apple also retains records related to communications between users and Apple customer service, including communications regarding a particular Apple device or service, and the repair history for a device.

28. Apple provides users with five gigabytes of free electronic space on iCloud, and users can purchase additional storage space. That storage space, located on servers controlled by Apple, may contain data associated with the use of iCloud-connected services, including: email (iCloud Mail); images and videos (iCloud Photo Library, My Photo Stream, and iCloud Photo Sharing); documents, spreadsheets, presentations, and other files (iWork and iCloud Drive); and web browser settings and Wi-Fi network information (iCloud Tabs and iCloud Keychain). iCloud can also be used to store iOS device backups, which can contain a user's photos and videos, iMessages, Short Message Service ("SMS") and Multimedia Messaging Service ("MMS") messages, voicemail messages, call history, contacts, calendar events, reminders, notes, app data and settings, Apple Watch backups, and other data. Records and data associated with third-party apps may also be stored on iCloud; for example, the iOS app for WhatsApp, an instant messaging service, can be configured to regularly back up a user's instant messages on iCloud Drive. Some of this data is stored on Apple's servers in an encrypted form but can nonetheless be decrypted by Apple.

29. In my training and experience, evidence of who was using an Apple ID and from where, and evidence related to criminal activity of the kind described above, may be found in the files and records described above. This evidence may establish the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or, alternatively, to exclude the innocent from further suspicion. As described above, the historical location information and other records shows that Jaquan Moore traveled from Minnesota to Kenosha, Wisconsin on August 24, 2020. After his arrest, Moore called Jada Deel—the same person listed as the subscriber for Moore's cell phone number and had conversations on jail calls, where Moore admitted to criminal activity and asked Deel to delete records and information relevant to this investigation.

30. For example, the stored communications and files connected to an Apple ID may provide direct evidence of the offenses under investigation. Based on my training and experience, instant messages, emails, voicemails, photos, videos, and documents are often created and used in furtherance of criminal activity, including to communicate and facilitate the offenses under investigation. Based on the information described above, it is probable that communications, including instant messages, emails, voicemails, photos, videos, and call records, from Moore, including those before, during, and after the Charlie's 10th Hole bar arson and CVS pharmacy burglary, are likely to be contained in the records and information associated with the accounts listed in Attachment A, along with evidence of any attempt to delete records and information relating to this investigation and Moore's whereabouts before he traveled to Kenosha on August 24, 2020.

31. In addition, the user's account activity, logs, stored electronic communications, and other data retained by Apple can indicate who has used or controlled the account. This "user

attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, subscriber information, email and messaging logs, documents, and photos and videos (and the data associated with the foregoing, such as geo-location, date and time) may be evidence of who used or controlled the account at a relevant time. As an example, because every device has unique hardware and software identifiers, and because every device that connects to the Internet must use an IP address, IP address and device identifier information can help to identify which computers or other devices were used to access the account. Such information also allows investigators to understand the geographic and chronological context of access, use, and events relating to the crime under investigation. In the investigation of an arson during a riot, this information is all the more important to corroborate who is using the phone and participating in communications.

32. Account activity may also provide relevant insight into the account owner's state of mind as it relates to the offenses under investigation. For example, information on the account may indicate the owner's motive and intent to commit a crime (e.g., information indicating a plan to commit a crime), or consciousness of guilt (e.g., deleting account information in an effort to conceal evidence from law enforcement).

33. Other information connected to an Apple ID may lead to the discovery of additional evidence. For example, the identification of apps downloaded from App Store and iTunes Store may reveal services used in furtherance of the crimes under investigation or services used to communicate with co-conspirators. In addition, emails, instant messages, Internet activity, documents, and contact and calendar information can lead to the identification of co-conspirators and instrumentalities of the crimes under investigation. In this case, it may also allow investigators

to pursue other investigative leads about the three-car caravan that traveled from Minnesota to Kenosha, Wisconsin to participate in the riots, including the methods of communication.

34. A preservation letter, pursuant to Title 18, United States Code, Section 2703(f), was sent to Apple requesting the preservation of all stored communications, records, and other evidence relating to the accounts listed in Attachment A (except for the Yahoo email address) on August 30, 2020. On September 1, 2020, Apple provided a preliminary response suggesting that they have preserved the records and information for the accounts listed in Attachment A.

35. Therefore, Apple's servers are likely to contain stored electronic communications and information concerning subscribers and their use of Apple's services. In my training and experience, such information may constitute evidence of the crimes under investigation including information that can be used to identify the account's user or users.

## INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED

36. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the warrant to require Apple to disclose to the government copies of the records and other information (including the content of communications and stored data) particularly described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

## CONCLUSION

37. Based on the forgoing, I request that the Court issue the proposed search warrant.

38. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant. The government will execute this warrant by

serving the warrant on Apple. Because the warrant will be served on Apple, who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

## ATTACHMENT A

### Property to Be Searched

This warrant applies to information associated with the Apple IDs and Apple iCloud accounts associated with the following information, that is stored at premises owned, maintained, controlled, or operated by Apple Inc., a company headquartered at Apple Inc., One Apple Park Way, Cupertino, California 95014.

**Account 1:**

- Name: Jaquan D. Moore
- Date of birth: 10/04/1997
- Address: 119 16th Avenue NE, Minneapolis, Minnesota 55413

**Account 2:** Phone: (612) 802-8429

**Account 3:** JDEEL08@ICLOUD.COM

**Account 4:** JDEEL08@YAHOO.COM

**Account 5:** Phone: (612) 513-9131

## ATTACHMENT B

### Particular Things to be Seized

### I. Information to be disclosed by Apple

To the extent that the information described in Attachment A is within the possession, custody, or control of Apple, regardless of whether such information is located within or outside of the United States, including any messages, records, files, logs, or information that have been deleted but are still available to Apple, or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Apple is required to disclose the following information to the government, in unencrypted form whenever available, for each account or identifier listed in Attachment A:

a. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers, email addresses (including primary, alternate, rescue, and notification email addresses, and verification information for each email address), the date on which the account was created, the length of service, the IP address used to register the account, account status, associated devices, methods of connecting, and means and source of payment (including any credit or bank account numbers);

b. All records or other information regarding the devices associated with, or used in connection with, the account (including all current and past trusted or authorized iOS devices and computers, and any devices used to access Apple services), including serial numbers, Unique Device Identifiers ("UDID"), Advertising Identifiers ("IDFA"), Global Unique Identifiers ("GUID"), Media Access Control ("MAC") addresses, Integrated Circuit Card ID numbers ("ICCID"), Electronic Serial Numbers ("ESN"), Mobile Electronic Identity Numbers ("MEIN"), Mobile Equipment Identifiers ("MEID"), Mobile Identification Numbers ("MIN"), Subscriber Identity Modules ("SIM"), Mobile Subscriber Integrated Services Digital Network Numbers

("MSISDN"), International Mobile Subscriber Identities ("IMSI"), and International Mobile Station Equipment Identities ("IMEI");

c. The contents of all emails associated with the account from August 22, 2020 through September 1, 2020, including stored or preserved copies of emails sent to and from the account (including all draft emails and deleted emails), the source and destination addresses associated with each email, the date and time at which each email was sent, the size and length of each email, and the true and accurate header information including the actual IP addresses of the sender and the recipient of the emails, and all attachments;

d. The contents of all instant messages associated with the account from August 22, 2020 through September 1, 2020, including stored or preserved copies of instant messages (including iMessages, SMS messages, and MMS messages) sent to and from the account (including all draft and deleted messages), the source and destination account or phone number associated with each instant message, the date and time at which each instant message was sent, the size and length of each instant message, the actual IP addresses of the sender and the recipient of each instant message, and the media, if any, attached to each instant message;

e. The contents of all files and other records stored on iCloud, including all iOS device backups, all Apple and third-party app data, all files and other records related to iCloud Mail, iCloud Photo Sharing, My Photo Stream, iCloud Photo Library, iCloud Drive, iWork (including Pages, Numbers, Keynote, and Notes), iCloud Tabs and bookmarks, and iCloud Keychain, and all address books, contact and buddy lists, notes, reminders, calendar entries, images, videos, voicemails, device settings, and bookmarks;

f. All activity, connection, and transactional logs for the account (with associated IP addresses including source port numbers), including FaceTime call invitation logs, messaging and

query logs (including iMessage, SMS, and MMS messages), mail logs, iCloud logs, iTunes Store and App Store logs (including purchases, downloads, and updates of Apple and third-party apps), My Apple ID and iForgot logs, sign-on logs for all Apple services, Game Center logs, Find My iPhone and Find My Friends logs, logs associated with web-based access of Apple services (including all associated identifiers), and logs associated with iOS device purchase, activation, and upgrades;

g. All records and information regarding locations where the account or devices associated with the account were accessed, including all data stored in connection with Location Services, Find My iPhone, Find My Friends, and Apple Maps;

h. All records pertaining to the types of service used;

i. All records pertaining to communications between Apple and any person regarding the account, including contacts with support services and records of actions taken; and

j. All files, keys, or other information necessary to decrypt any data produced in an encrypted form, when available to Apple (including, but not limited to, the keybag.txt and fileinfolist.txt files).

Apple is hereby ordered to disclose the above information to the government within **10 DAYS** of issuance of this warrant.

## II. Information to be seized by the government

All information described above in Section I that constitutes evidence of travel in interstate commerce or use of a facility of interstate commerce with intent to riot, in violation of Title 18, United States Code, Section 2101, conspiracy to commit arson, in violation of Title 18, United States Code, Section 844(m), arson of commercial property, in violation of Title 18, United States Code, Section 844(i), burglary involving controlled substances, in violation of Title 18, United States Code, Section 2118(b), conspiracy to commit burglary involving controlled substances, in violation of Title 18, United States Code, Section 2118(d), false statements, in violation of Title 18, United States Code, Section 1001, and destruction, alteration, or falsification of records in federal investigations, in violation of Title 18, United States Code, Section 1519, involving Jaquan D. Moore, Jada Deel, and others since August 22, 2020, including, for each account or identifier listed on Attachment A, information pertaining to the following matters:

a. Preparatory steps taken in furtherance of these crimes;

b. Communications between Jaquan D. Moore, Jada Deel, Sherwin Pompey, James L. Fielders-Bowers, or others;

c. Relationship between Jaquan D. Moore, Jada Deel, Sherwin Pompey, James L. Fielders-Bowers, or others;

d. Information about the protests, riots, and civil unrest in the Kenosha, Wisconsin area occurring between August 23, 2020 and September 1, 2020;

e. Use, possession, custody, or control of the phone numbers 612-802-8429, 612-513-9131, 612-735-7080, and 262-653-6404;

f. Use, possession, custody, control, or location of the cellular device assigned International Mobile Subscriber Identity (IMSI) 310410231756520;

g. Use, possession, custody, control, or location of a Dodge Charger, a black Nissan Rogue SUV, and a white four-door Pontiac sedan

h. Accelerants or ignitable liquids (such as gasoline, kerosene, or other petroleum distillates), glass bottles, ignition devices (such as an improvised wick or towel), heat sources, and ignition sources (such as a lighter or matches);

i. Screwdriver, hammer, or other burglar's tools;

j. Appearance, clothing, and identity of Jaquan D. Moore on August 24, 2020;

k. Charlie's 10th Hole bar, located at 3805 22nd Avenue, Kenosha, Wisconsin;

l. CVS pharmacy, located at 3726 22nd Avenue, Kenosha, Wisconsin 53140;

m. Location, whereabouts, and patterns of travel of Jaquan D. Moore, Jada Deel, and others;

n. The identity of the person(s) who created or used the Apple ID, including records that help reveal the whereabouts of such person(s);

o. Any information about the existence, scope, or overt acts in furtherance of a conspiracy;

p. Any information related to motive, intent, or knowledge of the violations described above;

q. Any information related to the concealment or destruction of evidence of the violations described above;

r. Evidence indicating how and when the account was accessed or used, to determine the chronological and geographic context of account access, use and events relating to the crime under investigation and the account subscriber;

s. Any records pertaining to the means and source of payment for services (including any credit card or bank account number or digital money transfer account information);

t. Evidence indicating the subscriber's state of mind as it relates to the crime under investigation; and

u. Evidence that may identify any co-conspirators or aiders and abettors, including records that help reveal their whereabouts.